

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WALKME LTD., AN ISRAELI
COMPANY, et al.,

Plaintiffs,

v.

WHATFIX, INC., A DELAWARE
CORPORATION, et al.,

Defendants.

Case No. [23-cv-03991-JSW](#)

**ORDER GRANTING, IN PART, AND
DENYING, IN PART, MOTION TO
DISMISS SECOND AMENDED
COMPLAINT**

Re: Dkt. No. 115

Now before the Court for consideration is the motion to dismiss filed by Whatfix, Inc. (“WF Inc.”) and Whatfix PL (“WF PL”) (collectively “Whatfix”, unless otherwise noted). The Court has considered the parties’ papers, relevant legal authority, the record in this case, and has had the benefit of oral argument. The Court GRANTS, IN PART, AND DENIES, IN PART, Whatfix’s motion.

ANALYSIS

The facts underlying this dispute are set forth in the Court’s Order granting, in part, and denying, in part Whatfix’s motion to dismiss the First Amended Complaint. *See WalkMe, Ltd. v. Whatfix, Inc.*, 2024 WL 1221960, at *2 (N.D. Cal. Mar. 21, 2024). The Court will not repeat those allegations here. Plaintiffs, WalkMe Ltd. and WalkMe Inc. (collectively “WalkMe”), allege Whatfix violated the Defend Trade Secrets Act (“DTSA”) and California’s Uniform Trade Secrets Act (“CUTSA”) (the “Trade Secret Claims”). WalkMe bases those claims on what, for ease of reference, the Court will refer to as the “technical trade secrets” and the “business trade secrets.” WalkMe also alleges Whatfix violated the Computer Fraud and Abuse Act (“CFAA”) and

California’s Data Access and Fraud Act (“CDAFA”) (the “Access Claims”).

A. Applicable Legal Standards.

Whatfix moves to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6). Under that rule, a court’s inquiry “is limited to the allegations in the complaint, which are accepted as true and construed in the light most favorable to the plaintiff.” *Lazy Y Ranch Ltd. v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008). Even under the liberal pleading standard of Rule 8(a)(2), “a plaintiff’s obligation to provide ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and conclusions, and formulaic recitation of the elements of a cause of action will not do.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)). Pursuant to *Twombly*, a plaintiff cannot merely allege conduct that is conceivable but must instead allege “enough facts to state a claim to relief that is plausible on its face.” *Id.* at 570. “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556).

Some of WalkMe’s allegations are based “on information and belief,” which is permissible. *See Soo Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017). However, the facts must either be “peculiarly within the possession and control of the defendant” or the plaintiff’s belief must be supported “by factual information that makes the inference of culpability plausible.” *Id.* (quoting *Arista Records LLC v. Doe*, 604 F.3d 110, 120 (2d Cir. 2010)).

If the allegations are insufficient to state a claim, a court should grant leave to amend unless amendment would be futile. *See, e.g., Reddy v. Litton Indus. Inc.*, 912 F.3d 291, 296 (9th Cir. 1990); *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv., Inc.*, 911 F.2d 242, 246-47 (9th Cir. 1990). Where a plaintiff has previously amended and failed to correct deficiencies, the Court’s “discretion to deny leave to amend is particularly broad[.]” *Allen v. City of Beverly Hills*, 911 F.2d 367, 373 (9th Cir. 1990) (quoting *Ascon Props., Inc. v. Mobil Oil Co.*, 866 F.2d 1149, 1160 (9th Cir. 1989)).

//

//

B. WalkMe States Its Claims Against WF, Inc.

In its previous Order, the Court concluded that WalkMe’s allegations were sufficient to state a claim against WF Inc. based on conduct attributed to its employee Paula Prigge. *WalkMe*, 2024 WL 1221960, at *2 (“[T]here are allegations that WF Inc. had some involvement in the actions forming the trade secret and computer access claims.”). Although the Court concluded there were insufficient allegations to hold WF Inc. vicariously liable for WF PL’s acts, WalkMe clarifies that it does not premise its claims against WF Inc. on that theory. WalkMe continues to allege that Ms. Prigge accessed WalkMe’s system without authorization and learned “confidential details about WalkMe’s product and customized user experience ... underlying rule configurations driving the work flows and content displaced at customer deployment sites, downloaded PDFs, and accessed supporting documentation to gain a deeper understanding of WalkMe’s processes and product.” (SAC ¶¶ 34-35.) For the reasons discussed in the following sections, the Court concludes these allegations are sufficient to state a claim, in part, against WF Inc.

C. WalkMe States Claims for Misappropriation of the Technical Trade Secrets.

In order to state a claim under DTSA or CUTSA, WalkMe must allege: (1) it possessed trade secrets; (2) Whatfix misappropriated those trade secrets; and (3) Whatfix caused or threatened to cause WalkMe damage. *See Inteliclear, LLC v. ETC Global Holdings, Inc.*, 978 F.3d 653, 657-58 & n. 1 (9th Cir. 2020) (noting courts have analyzed claims together based on similarity of elements). The parties focus on the first two elements.

1. WalkMe Sufficiently Alleges It Possessed Trade Secrets.

The term “trade secrets” is defined broadly but consists of three essential components: “(1) information, (2) that is valuable because it is unknown to others, and (3) that the owner has attempted to keep secret.” *Id.* at 657. WalkMe is not required to disclose the details of its trade secrets but must include facts that “describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons ... skilled in the trade.” *Id.* at 658.

Whatfix argues that WalkMe still fails to identify the alleged trade secrets in sufficient

1 detail. In addition to the allegations contained in the body of the Second Amended Complaint
 2 (“SAC”), WalkMe attaches an exhibit that describes the alleged intrusions into the areas of its
 3 system that contain the alleged trade secrets. It also has videos of those intrusions, which it
 4 alleges show Whatfix employees engaging with the information that encompasses the technical
 5 trade secrets. WalkMe also attaches an exhibit about the documents and information its former
 6 employees and a former customer allegedly accessed before they went to work for Whatfix to
 7 support its allegations about the business trade secrets. (SAC, Exs. A-B.) The Court concludes
 8 that WalkMe does more than rely “catchall phrases” or on broad categories of information to
 9 describe the trade secrets. *Cf. IntelIClear*, 978 F.3d at 659 (holding that there were genuine issues
 10 of material fact about whether plaintiff identified trade secrets with particularity and that
 11 “reasonable jury could conclude that the uniquely designed tables, columns, account number
 12 structures, methods of populating table data, and combination or interrelation thereof, are
 13 protectable trade secrets”).

14 Whatfix also argues that WalkMe fails to allege facts that show it has taken reasonable
 15 measures to keep the relevant information secret. WalkMe alleges it has “legal restrictions setting
 16 out the limits and obligations of anyone given access to [its] system, password and security
 17 controls that require verification of each user’s identity, and operational controls that monitor and
 18 record usage of WalkMe’s platform.” (SAC ¶ 5; *see also id.* ¶¶ 27-28, 47-49 (describing other
 19 efforts to protect trade secrets including restricting access to certain information to “administrator”
 20 level users”); Dkt. No. 39-4, Master License and Services Agreement, ¶ 13.1 (stating information
 21 should be treated as confidential information if the information “reasonably should be understood
 22 to be confidential given the nature of the information and/or the circumstances of disclosure”).
 23 These are the types of actions that can satisfy this component of a trade secret. *See, e.g.,*
 24 *IntelIClear*, 978 F.3d at 660 (“Confidentiality provisions constitute reasonable steps to maintain
 25 secrecy.”); *DiscoverOrg Data, LLC v. Bitnine Glob., Inc.*, No. 19-cv-08098-LHK, 2020 WL
 26 6562333, at 5 (N.D. Cal. Nov. 9, 2020) (concluding that “password protection, restrictive license
 27 agreements, mail monitoring, and list protection” were types of steps that were sufficient on
 28 motion for default judgment to show “reasonable efforts” to maintain secrecy of trade secrets).

Whatfix's argument that the terms of WalkMe's agreements with its customers negate a finding of secrecy are arguments best raised in the context of summary judgment. *Cf. Hiossen, Inc. v. Kim*, No. 16-cv-01579 SJO (MRWx), 2016 WL 10987393, at *7 (C.D. Cal. Oct. 4, 2016) ("[W]hether a party claiming a trade secret undertook reasonable efforts to maintain secrecy is a question of fact[.]") (quoting *In re Providian Credit Card Cases*, 96 Cal. App. 4th 292, 306 (2002)).

Finally, Whatfix argues WalkMe disclosed the technical trade secrets on its website. WalkMe disputes the information that constitutes the trade secrets is included on its website. Based on its allegations about how Whatfix allegedly obtained the technical trade secrets, the Court concludes this argument raises factual disputes that cannot be resolved on a motion to dismiss.

Accordingly, the Court concludes that WalkMe sufficiently alleges it possessed trade secrets.

2. WalkMe Sufficiently Alleges Misappropriation of the Technical Trade Secrets.

Whatfix argues that WalkMe fails to allege misappropriation of either category of trade secrets. "Misappropriation" means:

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who--

(i) used improper means to acquire knowledge of the trade secret;

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was--

(I) derived from or through a person who had used improper means to acquire the trade secret;

(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret[.]

18 U.S.C. § 1839(5); *accord* Cal. Civ. Code § 3426.1(b). "Improper means" includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means[.]" 18 U.S.C. § 1839(6); *accord* Cal. Civ. Code §

1 3426.1(a).

2 WalkMe alleges Whatfix’s “business model is to provide cut-rate software that emulates
3 elements of WalkMe’s cutting-edge software, offering fewer features and lesser functionality but
4 at discount prices.” (SAC ¶ 8.) According to WalkMe, Whatfix could not undercut WalkMe on
5 price by legitimate means. Therefore, it used customer credentials to obtain access to the “inner
6 workings of WalkMe’s platform” to copy WalkMe’s product. (*Id.* ¶ 5; *see also id.* ¶¶ 9, 30-35.)¹
7 Whatfix argues that its employees were migrating customer data and that any access to the
8 WalkMe platform was legitimate. WalkMe alleges, however, that those employees “accessed
9 parts of the WalkMe system that contained no information relating to the customer[.]” (*Id.* ¶ 33;
10 *see also id.* ¶¶ 37-40.) The Court concludes that WalkMe sufficiently alleges misappropriation of
11 the technical trade secrets.

12 Turning to the business trade secrets, Whatfix argues the allegations are not sufficient to
13 plead that *it* acquired, used, or disclosed them. This theory is based on WalkMe’s allegations that
14 former employees and a former customer downloaded or emailed files containing the putative
15 trade secrets to themselves shortly before they joined Whatfix as employees. (SAC ¶¶ 65-68, 70,
16 80, 83, Ex. B.) “On information and belief,” these individuals and Whatfix “used WalkMe’s
17 confidential information gathered and/or retained by [the individual] to improve and inform”
18 Whatfix’s “sales strategies and customer facing communications ... sales and pricing strategies ...
19 [and] sales and product development strategies, including to specifically target WalkMe’s existing
20 customers.” (SAC ¶¶ 69, 75, 84.)

21 The mere fact that Whatfix hired these individuals is not sufficient to show that it acquired
22 trade secrets. *See, e.g., Carl Zeiss Meditec, Inc. v. Topcon Med. Sys., Inc.*, No. 19-cv-4162-SBA,
23 2019 WL 11499334, at *5 (N.D. Cal. Nov. 3, 2019); *Hooked Media Grp., Inc. v. Apple Inc.*, 55
24 Cal. App. 5th 323, 332 (2020). WalkMe argues it is reasonable to infer Whatfix acquired the
25 business trade secrets from the allegations that Whatfix targeted these individuals for their
26

27 ¹ WalkMe argues that paragraphs 117-119 and 128-129 support its allegations of
28 misappropriation. Those paragraphs are formulaic recitations of elements of the claim and without
reference to other facts they would be insufficient to state a claim under *Twombly*.

1 knowledge and from “the suspicious activities carried out by each individual ... shortly before
2 joining Whatfix.” (Opp. Br. at 12:20-21.) Prior to the hearing, WalkMe submitted additional
3 authorities that it argues are on point.

4 In *Auris Health, Inc. v. Noah Medical Corporation*, the court concluded that the plaintiff’s
5 “information and belief” allegations were supported by the “greater factual context” and were
6 sufficient to raise an inference of misappropriation. No. 22-cv-08073-AMO, 2023 WL 7284156,
7 at *4 (N.D. Cal. Nov. 3, 2023). That “factual context” included allegations that one defendant’s
8 download activity was “unlike any of his prior usage” of the plaintiff’s system. On his last day
9 with plaintiff, that defendant also erased information on a work hard drive by reformatting the
10 drive and did not tell the plaintiff. *Id.* The plaintiff also alleged another defendant had no
11 legitimate purpose for downloading information. That defendant later admitted he possessed some
12 of the alleged trade secrets. *Id.* at *5. WalkMe has not alleged that any of the former employees’
13 conduct was inconsistent with their prior download activities. More importantly, WalkMe has not
14 sued the former employees, which distinguishes this case from *Auris*. *Id.* at *3.

15 WalkMe also relies on *Allergan, Inc. v. Revance Therapeutics*, -- F. Supp. 3d --, 2024 WL
16 38289 (M.D. Tenn. Jan. 3, 2024). In that case the court concluded the allegations were sufficient
17 to allege the corporate defendant acquired information from two of plaintiff’s former employees
18 who allegedly accessed and downloaded the plaintiff’s trade secrets. Similar to the allegations in
19 *Auris*, one of those employees allegedly downloaded information “at a rate that was inconsistent
20 with her job responsibilities.” *Id.* at *4. Another employee, Shepherd, allegedly created a power
21 point exhibit that contained the plaintiff’s trade secrets while preparing for a job interview with the
22 defendant. *Id.* at *5. The plaintiff also alleged that the defendant placed these employees in
23 positions that would ensure it would benefit from the plaintiff’s trade secrets. *Id.*

24 The court concluded those allegations were sufficient to allege the defendant “at least
25 acquired” plaintiff’s trade secrets from both individuals. *Id.* at *9-10 (emphasis omitted).
26 However, the court concluded that the plaintiff did not sufficiently allege the defendant used the
27 information acquired from Shepherd because there were no allegations showing “similarity
28 between those trade secrets and the sales and marketing approach” taken by the defendant. *Id.* at

*13. The court also concluded the plaintiff failed to allege facts showing the defendant acquired Shepherd’s information “by improper means” because there were insufficient facts to support an inference that the defendant induced Shepherd to breach her duty of confidentiality to the plaintiff. For example, that there were no allegations that the terms of her employment “were contingent in some way on disclosing” the trade secrets. *Id.* at *15.

In *3D Systems, Inc. v. Wynne*, one of the defendants, Intrepid Automation (“Intrepid”), asserted a counterclaim for misappropriation of trade secrets against 3D Systems, Inc. (“3D”). No. 21-cv-01141-AGS-DDL, 2024 WL 1099677 (S.D. Cal. Mar. 12, 2024). Intrepid alleged that 3D sent an employee, Kuester, “to steal Intrepid’s trade secrets under the guise of seeking employment—or perhaps persuaded that employee to reveal those secrets after a legitimate job interview.” *Id.* at 4. 3D argued that the allegations were not sufficient because they were based on information and belief. The court, however, concluded the allegations were sufficient to raise a plausible inference that 3D acquired trade secrets. Those allegations included the fact that Kuester signed a non-disclosure agreement and, during a tour of Intrepid’s facility, saw “unreleased products and technologies” that constituted the trade secrets. Intrepid also included references to emails sent by 3D employees that included information 3D could only have learned from Kuester. *Id.* at *5.

The Court assumes for the sake of argument that WalkMe’s allegations are sufficient to allege that Whatfix at acquired the business trade secrets. However, the Court concludes the allegations are not sufficient to show it did so through “improper means.” There are no allegations that Whatfix was aware of the terms of WalkMe’s confidentiality agreements with its employees at the time it hired these individuals. WalkMe also does not allege that it alerted Whatfix to confidentiality agreements after they were hired or that it took any efforts to stop the alleged targeted recruitment of WalkMe personnel.²

Similarly, WalkMe does not allege that it reminded its employees of their duty to maintain the confidentiality of WalkMe’s trade secrets before they left its employ. *See, e.g., Bombadier*

² WalkMe did send Whatfix a cease and desist letter regarding the alleged misappropriation of technical trade secrets, which makes no reference to poaching employees. (*See* Dkt. No. 40-4.)

1 *Inc. v. Mitsubishi Aircraft Corp.*, 363 F. Supp. 3d 1169, 1175-76, 1182-83 (W.D. Wash. 2019)
 2 (finding that plaintiff alleged sufficient facts to show one corporate defendant acquired or used
 3 trade secrets but failed to plead knowledge where it did not show “communications with corporate
 4 executives to halt recruitment” were sent to that defendant); *Hiossen*, 2016 WL 10987393, at *2 .
 5 There also are no facts to support an inference that Whatfix provided these individuals with an
 6 incentive to breach any duty of confidentiality to WalkMe. *See, e.g., Allergan*, 2024 WL 38289,
 7 at *15; *3D Systems*, 2024 WL 1099677, at *4 (alleging Intrepid compensated Kuester enough to
 8 induce him to breach non-disclosure agreement). Further, unlike the allegations in *3D Systems*,
 9 WalkMe does not allege any facts that would support an inference Whatfix gained information
 10 about the business trade secrets that it could only have learned from the WalkMe employees and
 11 customer it hired. In addition, the Court finds the allegations are not sufficient to show Whatfix
 12 used the business trade secrets. For example, although allegations based on information and belief
 13 can be based on information exclusively within the defendant’s possession, WalkMe does not
 14 allege facts that suggest Whatfix’s adopted a corporate strategy that was similar to WalkMe’s
 15 strategies. *See Allergan*, 2024 WL 38289 at *13.

16 Accordingly, the Court DENIES the motion to dismiss the claims based on
 17 misappropriation of the technical trade secrets but GRANTS the motion to dismiss the claims
 18 based on misappropriation of the business trade secrets.

19 **D. WalkMe States a CFAA Claim, in Part.**

20 The Court previously found that WalkMe’s allegations were sufficient to state a claim
 21 under the CFAA based on conduct by Dipit Sharma. 2024 WL 1221960, at 5. Whatfix renews its
 22 motion to dismiss the claim in its entirety. Much of the conduct supporting WalkMe’s trade
 23 secrets claims is the same conduct that supports this claim. However, the CFAA was designed to
 24 prevent computer hacking and “is best understood as an anti-intrusion statute and not as a
 25 misappropriation statute.” *HiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1196 (9th Cir. 2022)
 26 (internal quotations and citations omitted).

27 WalkMe alleges that Whatfix “intentionally accesse[d] a computer without authorization or
 28

1 exceed[ed] authorized access” and obtained information from a protected computer.³ 18 U.S.C. §
 2 1030(a)(2). The Ninth Circuit interprets the “without authorization” provision to exclude claims
 3 based on violations of terms of use. *Id.* Under the CFAA, “exceeds authorized access” means “to
 4 access a computer with authorization and to use such access to obtain ... information in the
 5 computer that the accesser is not entitled so to obtain.” *Id.* § 1030(e)(6). The phrase “‘is not
 6 entitled so to obtain’ is best read to refer to information that a person is not entitled to obtain by
 7 using a computer that he is authorized to access.” *VanBuren v. United States*, 593 U.S. 374, 384
 8 (2021); *see also id.* at 390-91.

9 WalkMe argues that the amendments show this claim should not be limited to Mr.
 10 Sharma’s conduct. WalkMe includes allegations that other employees obtained credentials in
 11 violation of WalkMe’s contracts with its customers. (SAC ¶¶ 32, 43.) Those allegations allege a
 12 violation of terms of use and are not sufficient to state a claim under the CFAA. *United States v.*
 13 *Nosal*, 676 F.3d 854, 864 (9th Cir. 2012). WalkMe now includes allegations that Whatfix falsely
 14 told its customers it would use credentials for legitimate purpose and then used them to access
 15 areas of the system that it was not allowed to access. However, WalkMe alleges that
 16 administrative users had access to, as it argues, “the under-the-hood configurations at issue.”
 17 (Opp. Br. at 3:21.) It does not include allegations that Whatfix went into areas that WalkMe’s
 18 authorized users were unable to access. Accordingly, the Court concludes that with the exception
 19 of Mr. Sharma’s conduct after Whatfix’s work with its customer ended, WalkMe may allege that
 20 Whatfix accessed areas of its platform with an improper motive. That is not enough to state a
 21 claim under the CFAA. *VanBuren*, 593 U.S. at 378.

22 WalkMe also must be able to allege that Whatfix’s alleged violation caused damage or loss
 23 “during any 1-year period ... aggregating at least \$5,000 in value.” 18 U.S.C. §§
 24 1030(c)(4)(A)(i)(I), 1030(g). Whatfix argues WalkMe’s allegations of loss are not sufficient. The
 25 term “loss” means “any reasonable cost to any victim, *including the cost of responding to an*
 26 *offense, conducting a damage assessment*, and restoring the data, program, system, or information
 27

28 ³ Whatfix does not argue the facts are insufficient to support this element of the claim.

1 to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential
2 damages incurred because of interruption of service[.]” *Id.* § 1030(e)(11) (emphasis added). The
3 term “loss” focuses “on technological harms – such as the corruption of files – of the type
4 unauthorized users cause to computer systems and data.” *VanBuren*, 593 U.S. at 392.

5 WalkMe does not allege that when Whatfix’s employees accessed its platform the
6 employees deleted any data, corrupted any files, or caused any damage to the system. Instead,
7 WalkMe alleges its own “employees have spent many hours, totaling more than \$5,000 in costs,
8 analyzing, investigating, and responding to Defendants’ actions.” (SAC ¶ 142) The CFAA
9 includes the “cost of responding to an offense [and] conducting a damage assessment” in its
10 definition of “loss.” WalkMe argues these allegations are sufficient, relying on *Facebook, Inc. v.*
11 *Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016) (“*Power Ventures*”). In *Power Ventures*, it
12 was undisputed that the plaintiff’s “employees spent many hours, totaling more than \$5,000 in
13 costs, analyzing, investigating, and responding to Power’s actions,” which the court held
14 constituted “loss.” *Id.* at 1066. Subsequently, the Ninth Circuit concluded that the CFAA’s
15 reference “to damage assessments, data restoration, and interruption of service[,] clearly limits its
16 focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself.”
17 *Andrews v. Sirius XM Radio, Inc.*, 932 F.3d 1253, 1262-63 (9th Cir. 2019).

18 Several courts within this District have considered allegations of loss that are similar to
19 WalkMe’s allegations. For example, WalkMe relies on *Facebook, Inc. v. Holper*, No. 20-cv-
20 6023-JCS, 2022 WL 17167958 (N.D. Cal. Sept. 27, 2022) (“*Holper*”). In *Holper*, the plaintiff
21 moved for default judgment. When the court analyzed the sufficiency of the plaintiffs’ claim
22 under the CFAA, it concluded the plaintiff’s allegations of costs to investigate and stop the
23 defendant’s improper access to the its platform were “materially indistinguishable” from the facts
24 supporting loss in *Power Ventures*. Therefore, the court found that factor weighed in favor of
25 granting the motion. *Id.* at *8. In another case, the court concluded that allegations of costs
26 incurred to “devote personnel, resources, and time to identifying and investigating [the
27 defendant’s] attacks and exploits,” to “develop[] and deploy[] security patches and software
28 upgrades,” and to increase “security measures to detect and prevent future attacks” were sufficient

1 to allege loss under the CFAA. *Apple Inc. v. NSO Grp. Tech. Ltd.*, No. 21-cv-9078-JD, 2024 WL
2 251448, at *4 (N.D. Cal. Jan. 23, 2024).

3 Whatfix relies on *X Corp. v. Center for Countering Digital Hate, Inc.*, – F. Supp. 3d –,
4 2024 WL 1246318 (N.D. Cal. Mar. 25, 2024). In that case, the plaintiff alleged the defendants
5 gained improper access to the plaintiff’s protected data and then used that data to publish articles
6 and reports to suggest the X platform was “overwhelmed with harmful content.” *Id.* at *1 The
7 purported motive for this conduct was to convince companies to stop advertising on X. *Id.* The
8 plaintiff alleged it spent over \$5,000 “on internal investigations, employee resources, and time to
9 assist in those investigations.” *Id.* at *23. The court distinguished *Holper* on the basis that the
10 plaintiff’s employees did not try to disable accounts or block defendant’s access to the data. *Id.* at
11 *24. The court concluded that plaintiff’s allegations of loss were “incurred not ... to assess the
12 breached system but to assess” the plaintiff’s damages and were not losses that are cognizable
13 under the CFAA. *Id.* at *25 (cleaned up and quoting *Fraser v. Mint Mobile, LLC*, No. 22-cv-
14 00138-WHA, 2022 WL 2391000, at *2 (N.D. Cal. July 21, 2022)).

15 In *Fraser*, which involved a data breach, the plaintiff alleged that cyber criminals obtained
16 his personal information and used that information to hack into and steal funds from his crypto
17 currency account. *Id.* at *1. The court concluded the plaintiff’s allegations that he “hired a
18 cryptographic expert to trace blockchain movements of [his] stolen assets” were “not related to
19 remedying technological harms inflicted on the breached computer or system. Instead, they
20 flowed from the use of unlawfully obtained information.” *Id.*

21 These authorities show that when courts have found when a plaintiff premises damage or
22 loss from responding to an offense or from doing a damage assessment was sufficient to show loss
23 under the CFAA, the underlying facts show that the plaintiff took actions to prevent the type of
24 intrusion the CFAA was enacted to prevent. Here, WalkMe alleges that when it discovered an
25 initial unauthorized intrusion, it spent time to investigate and document subsequent intrusions. In
26 addition, as in *Holper*, it alleges it suspended one of the “fake” accounts and sent Whatfix a cease
27 and desist letter. (SAC ¶¶ 34, 36, 44, 61; *see also* Dkt. No. 40-4.) The Court concludes WalkMe
28 has done just enough to plead loss.

Accordingly, the Court grants, in part, and denies, in part Whatfix's motion to dismiss the CFAA claim.

E. WalkMe States a Claim for Violations of Section 502.

The Court previously concluded that WalkMe's allegations were sufficient to state a claim under Section 502: namely knowing access and improper use of information. *WalkMe*, 2024 WL 1221960, at *6 (citing *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015)). Whatfix argues this claim should be limited to the allegations regarding Dipit Sharma. WalkMe argues that its allegations show other Whatfix employees also made improper use of WalkMe information. The Court agrees. WalkMe alleges that Whatfix employees gained access to the trade secrets and improperly used that information to "improve Whatfix's copycat products including by making it more attractive to potential customers by undercutting WalkMe on price (something they would not be able to do if they were investing in a comparable level of research and development as WalkMe)." (SAC ¶ 30). The Court concludes WalkMe's allegations are sufficient to state a claim. *See Christensen*, 828 F.3d at 789 ("A plain reading of the statute demonstrates that its focus is on unauthorized taking or use of information.").

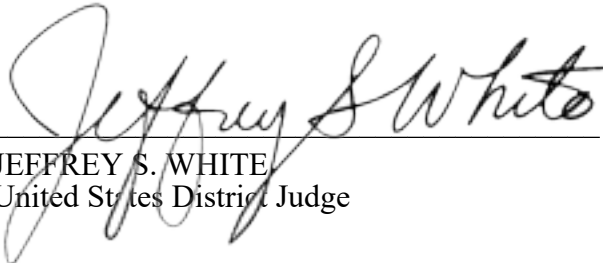
Accordingly, the Court DENIES Whatfix's motion to dismiss the Section 502 claim.

CONCLUSION

For the foregoing reasons, the Court GRANTS, IN PART, AND DENIES, IN PART, Whatfix's motion to dismiss. Whatfix shall file an answer by July 30, 2024. The Court lifts the stay on discovery.

IT IS SO ORDERED.

Dated: July 9, 2024


JEFFREY S. WHITE
United States District Judge